THE UNIVERSITY OF TEXAS-PAN AMERICAN
OFFICE OF AUDITS & CONSULTING SERVICES

LAPTOP ENCRYPTION

Report No. 13-14
September 3, 2013

Dr. Robert S. Nelsen, President
The University of Texas-Pan American
1201 W. University Drive
Edinburg, TX 78539

Dear Dr. Nelsen,

As part of our fiscal year 2013 Audit Plan, we completed an externally required audit of Laptop Encryption. The objectives of this audit were to determine whether laptop inventory at UTPA was complete, accurate, and up-to-date; and to determine whether all UTPA laptops were properly encrypted or exempted from encryption. The scope of this audit included all UTPA laptop computers.

We performed audit procedures that included interviewing employees, obtaining a list of laptops in inventory, obtaining a list of encrypted laptops, and inspecting a sample of encrypted laptops.

We concluded that the measures taken to encrypt University laptops were effective and operating as intended. The University’s inventory was complete and accurate and the laptop encryption plan was effective to provide reasonable assurance that all University owned laptops were identified and encrypted. The Information Technology Division and the Office of Privacy and Security successfully deployed its laptop encryption plan; however, we identified opportunities for improvement. The detailed report is attached for your review.

We appreciate the courtesy and cooperation received from management and staff during our audit.

Sincerely,

Eloy R. Alaniz, Jr., CPA, CIA, CISA
Executive Director of Audits, Compliance & Consulting Services
# Table of Contents

EXECUTIVE SUMMARY .................................................. 1

BACKGROUND .............................................................. 2

AUDIT OBJECTIVE ......................................................... 3

AUDIT SCOPE AND METHODOLOGY ..................................... 3

AUDIT RESULTS ............................................................ 3

CONCLUSION ................................................................. 8
EXECUTIVE SUMMARY

Protecting portable devices has been a priority of The University of Texas System (UTS). In 2007, UTS issued a bulletin, “Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices (SPB-1).” This policy provided the foundation for the laptop encryption memoranda issued by the Executive Vice Chancellors in Health Affairs and Academic Affairs to all UTS institutional presidents. Within each memorandum, the Executive Vice Chancellors asked each campus to encrypt all University laptop computers, including personal computers used for any University business, by August 31, 2012.

The objectives of this audit were to determine whether laptop inventory at UTPA was complete, accurate, and up-to-date; and to determine whether all UTPA laptops were properly encrypted or exempted from encryption.

We concluded that the measures taken to encrypt University laptops were effective and operating as intended. The University’s inventory was complete and accurate and the laptop encryption plan was effective to provide reasonable assurance that all University owned laptops were identified and encrypted. The University deployed a new process to centrally encrypt new laptops. While the Information Technology Division and the Office of Privacy and Security successfully deployed its laptop encryption plan, we observed the following:

- 10 pre-approved laptop purchases were miscoded with the wrong accounting code preventing them from being approved by Assets Management (AM) and captured in the University’s Fixed Asset System.

- The University does not have a formal process to identify and list personally owned laptops used to conduct University business.

- 22 encrypted laptops managed by SecureDoc, the new encryption management system, had not established connection with the SecureDoc server in several months.
BACKGROUND

In 2007, The University of Texas System (UTS) issued a bulletin, “Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices (SPB-1),” which lays out the basic expectations and requirements for the encryption of laptop computers across the UT System. However, in 2007 no single solution was available to encrypt all laptop platforms and many institutions did not readily adopt a solution. Since 2007, UT System has experienced several incidents of lost or stolen laptops containing confidential or sensitive data. As a result, the Executive Vice Chancellors in Health and Academic Affairs issued a memorandum to each institutional president, which required all institutions to report their current state of laptop encryption and their respective plans to encrypt all laptops, including personal computers used for any University business, by August 31, 2012. The memoranda required each institution to report this information by July 1, 2012.

UTPA reported the following:

- An inventory of 1930 institutionally owned laptops
- 161 encrypted laptops
- Plans to announce its own laptop encryption process when the Executive Vice Chancellor’s memorandum was received.
- The need to encrypt 50 laptops per day and the steps necessary to accomplish this rate.
  - Direct user involvement – laptop users have the ability to download the WinMagic encryption application from the myUTPA software portal along with instructions on how to successfully complete the process. Incentives are being provided to users to select this method.
  - Help Desk personnel will be available to assist users who may not be comfortable encrypting their own computers.
  - Mass encryption efforts will be held at a central location on campus where laptop owners can bring their computers in to get assistance or drop off the laptop to be encrypted by technical staff.
  - Additional technical staff will be hired to assist with direct outreach efforts.
  - For dual-boot and unsupported operating systems, hardware encrypted hard drives are being procured to enable the accountability functionality in the WinMagic console. Additionally, WinMagic licenses are being procured to provide coverage for all identified computers.
  - Computers that connect to the University’s Virtual Private Network (VPN) from off campus will be scanned for encryption software with our Network Access Control device. Connection access will depend on whether the computers are encrypted.
- Request encryption exceptions for certain computers that have limited risk of containing confidential data or being lost or stolen.

The University recently developed a new process to ensure that all newly purchased laptops are encrypted. All laptops will be encrypted in a staging area in the Central Receiving Warehouse prior to department delivery.
AUDIT OBJECTIVE

The objectives of this audit were to determine whether laptop inventory at UTPA was complete, accurate, and up-to-date; and to determine whether all UTPA laptops were properly encrypted or exempted from encryption.

AUDIT SCOPE & METHODOLOGY

The scope of this audit included all UTPA laptop computers. To accomplish the audit objectives, the following steps were taken:

- Reviewed the Executive Vice Chancellor’s Encryption Memorandum.
- Reviewed the system-wide encryption bulletin.
- Interviewed employees managing the laptop encryption process and laptop inventory.
- Obtained a list of all the laptops in inventory from Assets Management.
- Obtained a list of all encrypted laptops from the Office of Privacy and Security.
- Inspected a sample of encrypted laptops.

Our audit was conducted in accordance with guidelines set forth in The University of Texas System’s Policy 129 and The Institute of Internal Auditor’s International Standards for the Professional Practice of Internal Auditing. The audit was conducted between the months of March 2013 through July 2013.

AUDIT RESULTS

Laptop Inventory Population
The University employs several controls to ensure that the laptop inventory population is accurate, complete, and up-to-date. These controls include: pre-approved items through iShop, the University’s online shopping service, multiple purchase approvals, and Assets Management (AM) procedures.

University departments are encouraged to make their laptop purchases through iShop. iShop offers pre-approved laptops, however, these purchases do not have a default accounting code associated with the transaction. The proper accounting code is essential in capturing laptop purchases in inventory. Before laptop purchases are finalized in iShop, they are approved by representatives from information technology, information security and AM. Approval by AM’s staff ensures that laptop purchases are coded properly and added later to inventory.

After purchases are finalized, AM adds the laptop purchases to inventory each month during their mass additions. This process involves transferring purchases accounted for in the University’s projects management system to the Fixed Assets module. In order to ensure the accuracy of this process, AM performs weekly reconciliations of purchases against assets received prior to the monthly mass additions process. These reconciliations involve capturing and correcting discrepancies, identifying purchases with asset numbers, and determining the
location and the asset category of new assets. The asset category describes all purchases including laptops. Any discrepancies in these reconciliations are corrected by AM. In some instances, require the assistance of other departments, such as Accounts Payable and Procurement Management to make needed corrections.

To determine whether these controls ensure that the laptop inventory was complete and accurate, we selected and tested a sample of 40 purchases from a report of equipment purchases. The report included a total of 111 laptops purchased during the period of 9/1/2012 thru 4/22/2013. We determined that these controls were adequate and working as intended; however, we identified some areas for improvement. We identified 10 (or 25%) of the purchases tested were not approved by AM. These purchases were not approved by AM because the accounting codes in iShop were incorrect; however, the weekly reconciliations captured and included these items in inventory.

The Executive Vice Chancellor’s memorandum asks to encrypt all University laptop computers, including personally owned computers used for any University business. We determined that the University does not have a formal process to identify and list personally owned laptops that are used to conduct University business. Employees are responsible for contacting the Office of Privacy and Security about their use of personally owned laptops to conduct University business. They must encrypt their laptops on their own or request assistance from the University Help Desk.

In accordance with UTS 165, section 11.3.3 sensitive digital data must not be stored on UT System or personal computers or other electronic devices (e.g. laptop, hand-held device, flash drives, or other portable computing devices) unless;

- It is secured against unauthorized access in accordance with this policy;
- It will not compromise business or research efforts or privacy interests if lost or destroyed; and
- The entity has specific procedures in place that address this section.

**Recommendations:**

1. Procurement Management should ensure that all pre-approved laptops in iShop have an appropriate default accounting code that will capture these assets in inventory.

2. The Office of Privacy and Security (OCISO) should develop a process to create and maintain a list of personally owned laptops used to conduct University business. This list should include information on the encryption status of each of these laptops.
Management’s Responses:

1. Procurement Management is working with the iShop vendor to tie back pre-approved laptops to the accounting codes or UNSPC (United Nations Standard Products and Services Code) controlled assets.

   **Implementation Date:** January 31, 2014

2. Currently there is no realistic way to enforce this requirement. It would require users to voluntarily report the use of their personal computer for University business. Since University data could be removed via removable media and transported home without the knowledge of the OCISO staff we cannot force user registration or the out of band transfer of information.

   OCISO will continue to educate end users on the proper handling and protection of sensitive University data through outreach and training.

   OCISO will send out a reminder of the personal laptop encryption requirement and licensing that is available for the SecureDoc and Bitlocker (encryption software) products at no charge to the user.

   As capabilities improve OCISO will seek out ways to implement technological solutions to address this issue more holistically.

   **Implementation Date:** September 15, 2013

**Laptop Encryption**

We obtained a report of all University laptops from AM. The report included 1,815 laptops. We selected a test sample of 90 laptops, representing 5% of the population to verify that the laptops were encrypted. This sample included laptops from areas with the following risks factors:

- Number of records within a department
- FERPA (Family Educational Rights and Privacy Act)
- HIPAA (Health Insurance Portability and Accountability Act)
- PCI-DSS (Payment Card Industry – Data Security Standard)
- Other confidential information and regulations

The laptop encryption test was performed using SecureDoc, an encryption management system. The laptops’ asset numbers were used to identify the laptops in SecureDoc. All laptops managed by SecureDoc have full disk encryption.
A summary of the laptop encryption test results is included in the table below.

<table>
<thead>
<tr>
<th>Qty</th>
<th>*Percentage</th>
<th>Tag Numbers</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>58%</td>
<td>55647, 56654, 57894, 57902, 57919, 58353, 58749, 58999, 59006, 59010, 59160, 59477, 59519, 59929, 63509, 63510, 63537, 63607, 63608, 64257, 64266, 64268, 64425, 64541, 64625, 64801, 64899, 64996, 65068, 65143, 65757, 65765, 65936, 66028, 66037, 66350, 66568, 66737, 67344, 67396, 67415, 67563, 67634, 67635, 67701, 67953, 67970, 68245, 68247, 69346, 70180, 70519</td>
<td>Laptops were <strong>encrypted</strong>. Reported current connections to SecureDoc server.</td>
</tr>
<tr>
<td>22</td>
<td>24%</td>
<td>56632, 56643, 57603, 57628, 58077, 58494, 58643, 58645, 59011, 59156, 59388, 59525, 63006, 64221, 64573, 64579, 64774, 64922, 65104, 66023, 68967, 69179</td>
<td>Laptops were <strong>encrypted</strong>, but reported last connection to SecureDoc server before 12/31/2012.</td>
</tr>
<tr>
<td>1</td>
<td>1%</td>
<td>64540</td>
<td>Laptop was <strong>encrypted</strong>, but not found in encrypted report.</td>
</tr>
<tr>
<td>1</td>
<td>1%</td>
<td>59925</td>
<td>Laptop was <strong>encrypted</strong>. Encryption software was running on laptop, but laptop did not report in SecureDoc.</td>
</tr>
<tr>
<td>4</td>
<td>4%</td>
<td>50288, 56789, 57591, 58410</td>
<td>Laptops were in the process of being sent to surplus.</td>
</tr>
<tr>
<td>3</td>
<td>3%</td>
<td>44831, 49007, 58402</td>
<td>Laptops were reported as missing.</td>
</tr>
<tr>
<td>3</td>
<td>3%</td>
<td>56021, 65469, 70181</td>
<td>Laptops did not work.</td>
</tr>
<tr>
<td>3</td>
<td>3%</td>
<td>68857, 68899, 69037</td>
<td>Tablets listed as laptops.</td>
</tr>
<tr>
<td>1</td>
<td>1%</td>
<td>68564</td>
<td>Laptop was replaced under warranty, replaced with laptop with tag number: 68565.</td>
</tr>
</tbody>
</table>

* Percentage of 90 laptops tested
Recommendation:

3. The Office of Privacy and Security (OCISO) should develop and implement a plan to monitor laptops that do not communicate with the SecureDoc server for prolonged periods of time.

Management’s Response:

3. Technically, any device that has reported into the console in an encrypted state should be encrypted since the user does not have the credentials to unencrypt the device.

However, OCISO is currently researching the feasibility of sending out reminders to program managers to connect laptops to maintain domain credentials, provide software updates and up to date encryption status.

Milestones for this project include:

a. Separate VPN or VLAN for offsite vendor connections (allows certain management ports to be opened to ensure regular communications with the offsite computer)

b. Accurate inventory of laptop devices by project manager and/or account manager (will allow for emailing the correct project manager and/or account manager)

c. Develop internal processes for determining subject laptops and notification methods.

Implementation Date: December 15, 2013

Exempted Laptops

Laptops exempt from encryption are permitted under the memoranda issued by the Executive Vice Chancellor. Exempt laptops are allowed only under circumstances that pose extremely low risk, are thoroughly documented, and must be individually authorized by the president of the institution. Currently, the University has 239 laptops that are exempt from encryption. The majority of these laptops are located in student labs in the Library and Education Building.

We obtained a copy of a memorandum approved by the president of laptops exempt from encryption from the Office of Privacy and Security. We selected a sample of 20 laptops, representing 8% of the population to test for confidential data. The exempted laptop test was performed using SENF, Sensitive Number Finder - software provided by UT System Information Technology Systems. SENF only searches for social security numbers and credit card numbers. However, the laptops tested used Deep Freeze software. This software protects the computer by deleting any data that has been downloaded and restoring the system to its original state once the user logs off the machine. We determined that none of the exempted laptops tested contained confidential data.
CONCLUSION

We concluded that the measures taken to encrypt University laptops were effective and operating as intended. The University’s inventory was complete and accurate and the laptop encryption plan was effective to provide reasonable assurance that all University owned laptops were identified and encrypted. The University deployed a new process to centrally encrypt new laptops. The Information Technology Division and the Office of Privacy and Security successfully deployed its laptop encryption plan. However, opportunities for improvement exist, such as, ensuring that all pre-approved laptops in iShop have appropriate accounting codes, creating and managing a list of personally owned laptops, and monitoring laptops that do not communicate regularly with the SecureDoc server.

Joe Gomez, MS
Information Systems Auditor III